1/5/2 (Item 2 from file: 351) **Links**
Fulltext available through: Order File History
Derwent WPI

0012930583 & & *Drawing available*
WPI Acc no: 2003-007169/**200301**
XRPX Acc No: N2003-006167
User identification method involves selecting print data in desired language, corresponding to input ID data of user and analyzing user voice while reading print data
Patent Assignee: SHARP KK (SHAF)
Inventor: AZUMA K

Patent Family (1 patents, 1 & countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
JP 2002304379	A	20021018	JP 2001107846	A	20010405	200301	B

Priority Applications (no., kind, date): JP 2001107846 A 20010405

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
JP 2002304379	A	JA	9	7		

Alerting Abstract JP A
NOVELTY - A print data in desired language corresponding to input ID of a user, is selected by a server (2). The voice of the user while reading the print data, is analyzed and the analysis result is compared with a value stored in a storage medium, for identifying the user.
DESCRIPTION - An INDEPENDENT CLAIM is included for user identification system.
USE - For identifying user.
ADVANTAGE - Eliminates the need for carrying the credit cards and debit cards and increases the safety.
DESCRIPTION OF DRAWINGS - The figure shows the block diagram of the user identification system. (Drawing includes non-English language text).
2 Server

Title Terms /Index Terms/Additional Words: USER; IDENTIFY; METHOD; SELECT; PRINT; DATA; LANGUAGE; CORRESPOND; INPUT; ID; VOICE; READ

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G06F-0015/00	A	I		R	20060101
G06F-0021/20	A	I	F	R	20060101
G10L-0015/00	A	I	L	R	20060101
G10L-0015/06	A	I	L	R	20060101
G10L-0017/00	A	I	L	R	20060101
G06F-0015/00	C	I		R	20060101
G06F-0021/20	C	I	F	R	20060101
G10L-0015/00	C	I	L	R	20060101
G10L-0017/00	C	I	L	R	20060101

File Segment: EngPI; EPI;
DWPI Class: T01; T05; W04; P86
Manual Codes (EPI/S-X): T01-C08A; T01-J05B4P; T01-J18; T01-N01A1; T01-N02B1B; T05-L02; W04-V04A3

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－304379
（P2002－304379A）
(43)公開日　平成14年10月18日(2002.10.18)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)	
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｆ	５Ｂ０８５
Ｇ１０Ｌ	15/00		Ｇ１０Ｌ	3/00	５４５Ａ	５Ｄ０１５
	15/06				５２１Ｐ	
	17/00				５５１Ａ	

審査請求　未請求　請求項の数８　ＯＬ　（全９頁）

(21)出願番号　特願2001－107846(P2001－107846)

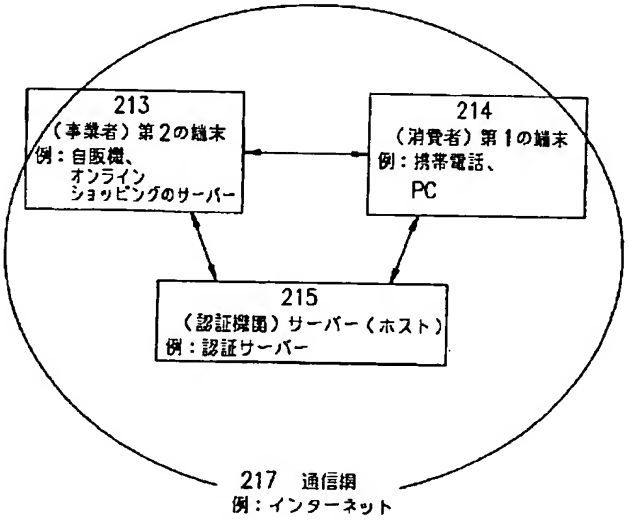
(22)出願日　平成13年４月５日(2001.4.5)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　東　賢一
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　100078282
弁理士　山本　秀策

Ｆターム(参考)　5B085 AE02 AE23 AE27
5D015 AA03 AA04 BB01 GG03 GG06 HH04

(54)【発明の名称】　個人認証方法および個人認証システム

(57)【要約】
【課題】　肉声に由来する声紋を個人認証のセキュリティの鍵として用いて、安全性を高めた個人認証方法および個人認証システムを提供する。
【解決手段】　被認証者単位で複数の言葉とそれらの言葉を被認証者に発声させたときの声紋データを予め記憶媒体にデータ２４２として記憶させておき、被認証者から入力されたＩＤデータに対応する複数の言葉のうちの任意の１つとそれに対応する声紋データを選択する。その言葉を被認証者に提示して発声させ、音声処理解析部２４４により声紋を解析して記憶媒体から選択した声紋データと照合する。両者が一致した場合にその被認証者を個人認証する。



【特許請求の範囲】

【請求項１】　被認証者から該被認証者のＩＤデータが認証手段に入力されたときに、

該認証手段は、被認証者単位で複数の言葉とそれらの言葉を被認証者に発声させたときの声紋データを予め記憶させておいた記憶媒体から、入力されたＩＤデータに対応する複数の言葉のうちの任意の１つとそれに対応する声紋データを選択して、

選択された言葉を被認証者に提示し、提示した言葉を被認証者に発声させて声紋を解析し、

解析結果と該記憶媒体から選択された声紋データとを照合して、両者が一致した場合にその被認証者を個人認証することを特徴とする個人認証方法。

【請求項２】　被認証者から該被認証者のＩＤデータが認証手段に入力されたときに、

該認証手段は、押複数の言葉を含む一覧データ表と被認証者の基本単位の声紋データを予め記憶させておいた記憶媒体から、該一覧データ表に含まれた複数の言葉のうちの任意の１つを選択すると共に、入力されたＩＤデータに対応する基本単位の声紋データを選択された言葉の配列に配列して声紋データを生成して、選択された言葉を被認証者に提示し、提示した言葉を被認証者に発声させて声紋を解析し、

解析結果と基本単位の声紋データから生成された声紋データとを照合して、両者が一致した場合にその被認証者を個人認証することを特徴とする個人認証方法。

【請求項３】　前記記憶媒体から複数の言葉のうちの任意の１つを選択する際に、前記認証手段の内部に格納されている乱数発生プログラムを用いる請求項１または請求項２に記載の個人認証方法。

【請求項４】　前記認証手段は、前記記憶媒体から複数の言葉のうちの任意の２つ以上を選択する請求項１乃至請求項３のいずれかに記載の個人認証方法。

【請求項５】　被認証者が操作する第１の操作手段と、該被認証者の認証を要求する第２の操作手段と、該被認証者の認証を行う認証手段とが通信網を介して接続されているシステムにおいて、

該認証手段は、少なくとも、被認証者単位で複数の言葉とそれらの言葉を被認証者に発声させたときの声紋データを予め記憶させておく記憶媒体と、

被認証者が第１の操作手段から入力した該被認証者のＩＤデータが通信網を介して該認証手段に伝えられたときに、該記憶媒体から、該ＩＤデータに対応する複数の言葉のうちの任意の１つとそれに対応する声紋データを選択して選択された言葉を該通信網を介して被認証者に提示する手段と、

提示した言葉を被認証者が発声した声を通信網を介して入力して声紋を解析する解析手段と、

解析結果と該記憶媒体から選択された声紋データとを照合する照合手段とを有することを特徴とする個人認証システム。

【請求項６】　被認証者が操作する第１の操作手段と、該被認証者の認証を要求する第２の操作手段と、該被認証者の認証を行う認証手段とが通信網を介して接続されているシステムにおいて、

該認証手段は、少なくとも、複数の言葉を含む一覧データ表と被認証者の基本単位の声紋データを予め記憶させておく記憶媒体と、

被認証者が第１の操作手段から入力した該被認証者のＩＤデータが通信網を介して該認証手段に伝えられたときに、該記憶媒体から、該一覧データ表に含まれた複数の言葉のうちの任意の１つを選択すると共に、入力されたＩＤデータに対応する基本単位の声紋データを選択された言葉の配列に配列して声紋データを生成して、選択された言葉を該通信網を介して被認証者に提示する手段と、

提示した言葉を被認証者が発声した声を通信網を介して入力して声紋を解析する解析手段と、

解析結果と基本単位の声紋データから生成された声紋データとを照合する照合手段とを有することを特徴とする個人認証システム。

【請求項７】　前記認証手段は、前記記憶媒体から複数の言葉のうちの任意の１つを選択する際に使用する乱数発生プログラムが内部に格納されている請求項５または請求項６に記載の個人認証システム。

【請求項８】　前記認証手段は、前記記憶媒体から複数の言葉のうちの任意の２つ以上を選択する請求項５乃至請求項７のいずれかに記載の個人認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、安全性を有する個人認証方法および個人認証システムに関し、特に、消費者側操作端末と事業者側操作端末と認証サーバー等のホストコンピューターとがインターネット等の通信網を介して接続されているシステムに好適な個人認証方法および個人認証システムに関する。

【０００２】

【従来の技術】従来、操作端末からホストコンピューターへのアクセス許可を得る方法として、暗証番号やパスワードを操作端末から入力して、ホストコンピューターが有するそれらのデータと照合することにより個人認証を行ってホストコンピューターへのアクセス許可を与えるものが知られている。

【０００３】しかし、近年、インターネット等のネットワークを利用した電子商取引が活発化するにつれて、より安全性の高い個人認証方法（セキュリティ）が求められている。

【０００４】このようなより安全性の高い個人認証方法として、例えば特開平１０－２１３０５号公報に記載されている認証方法が挙げられる。この公報の技術は、各

人固有の特徴である声紋、角膜紋、指紋、指の骨格および顔面パターンを個人認証（セキュリティ）の鍵として利用する電子商取引システムを構築し、商品購入者と商店との間に第３者機関としての認証サーバーを設けて、これをインターネット等の公共通信網により結び付けているものである。

【０００５】この従来技術は、図７に示すように、インターネット１０に接続され、商品購入希望者が購入したい商品の情報を受信する商店の端末装置１１と、商品購入希望者から、その商品購入希望者固有の身体的特徴の情報とこれを検索するための検索コードとを商品購入希望についての情報に付加して認証サーバー（ホストコンピューター）１３に送信する情報処理装置１２と、認証を行う認証サーバー１３からシステムが構成される。

【０００６】認証サーバー１３は、商品購入希望者固有の身体的特徴の情報を、被照合情報として検索コードに対応させて記憶しているメモリ１３ｅを有し、情報処理装置１２から送信された商品購入希望者の身体的特徴の情報と検索コードと商品購入希望についての情報とを受信して、受信した身体的特徴の情報と、検索コードにより検索した身体的特徴の情報とが一致しているか否かを判定する。そして、それらが一致しているときに本人であるという認証を行い、商店の端末装置１１に商品購入希望についての情報を送信する。ここでは、購入者固有の身体的特徴として、声紋、角膜紋、指紋、指の骨格および顔面パターンが例示されている。

【０００７】なお、この図７において、１４は情報処理装置１２のＭＰＵであり、１５は電子取引処理プログラム１５ａ、認証通信処理プログラム１５ｂ、暗号化処理プログラム１５ｃおよび認証データ生成プログラム１５ｄ等を格納したメモリであり、１６はメモリ１６ａを有する音声入力装置であり、１７はマイクロホンである。また、１３ａは認証サーバー１３において送信されたデータを復元する解読回路であり、１３ｂは特徴抽出処理回路であり、１３ｃはＭＰＵであり、１３はＩＤパターン記憶部１３１、標準ＩＤパターンテーブル１３２、ＤＰマッチング処理プログラム１３３、データ送信プログラム１３４等を有するメモリである。

【０００８】

【発明が解決しようとする課題】上述した特開平１０－２１３０５号公報の従来技術において、利用される個人認証（セキュリティ）の鍵のうち、角膜紋、指紋、指の骨格および顔面パターンについては、これらのデータが認証サーバー１３内のメモリに格納されている。これらの格納データ、または情報処理装置１２から取り込んで認証サーバー１３に転送中のデータを、一旦何らかの手法により第三者に盗み取られた場合、その身体的特徴は個人固有のものであるが故に、セキュリティの鍵を変更することはほとんど不可能である。

【０００９】また、上記従来技術においては、上記データの暗号化によるセキュリティ向上についても考慮されている。しかし、その暗号が解読された場合には、やはり各人固有の身体的特徴であるが故に、、セキュリティの鍵を変更することは困難である。

【００１０】さらに、上記従来技術において、もう１つのセキュリティの鍵である声紋については、商品購入希望者が認証を受けるときに自らが選んだ暗証コードと音声ＩＤデータ（肉声または肉声に由来する声紋）を使用する。しかし、この方法では、悪意を有する者に暗証コードを盗み取られ、さらに音声ＩＤデータを録音されてしまうおそれがある。例えば、操作端末からの入力が公共の場所、例えばデパートメントストアにおいてショッピングを行っている場合や自動販売機からの商品購入時における利用を考えると、その公共性の故に上記問題が重要になる。

【００１１】従って、上記従来技術は、安全性の高い個人認証システムであるとは言えない。

【００１２】本発明は、肉声に由来する声紋を個人認証のセキュリティの鍵として用い、さらに安全性を高めた個人認証方法および個人認証システムを提供することを目的とする。

【００１３】

【課題を解決するための手段】本発明の個人認証方法は、被認証者から該被認証者のＩＤデータが認証手段に入力されたときに、該認証手段は、被認証者単位で複数の言葉とそれらの言葉を被認証者に発声させたときの声紋データを予め記憶させておいた記憶媒体から、入力されたＩＤデータに対応する複数の言葉のうちの任意の１つとそれに対応する声紋データを選択して、選択された言葉を被認証者に提示し、提示した言葉を被認証者に発声させて声紋を解析し、解析結果と該記憶媒体から選択された声紋データとを照合して、両者が一致した場合にその被認証者を個人認証することを特徴とする。

【００１４】上記方法によれば、消費者を認証するための鍵となる「言葉」を、例えば日時等により認証手段側で任意に変えることができ、デパートメントストアや商店、自動販売機、銀行のＡＴＭ等の公共の場所であって、悪意を有する者が存在するおそれがある場所においても、高いセキュリティを維持することが可能である。

【００１５】本発明の個人認証方法は、被認証者から該被認証者のＩＤデータが認証手段に入力されたときに、該認証手段は、複数の言葉を含む一覧データ表と被認証者の基本単位の声紋データを予め記憶させておいた記憶媒体から、該一覧データ表に含まれた複数の言葉のうちの任意の１つを選択すると共に、入力されたＩＤデータに対応する基本単位の声紋データを選択された言葉の配列に配列して声紋データを生成して、選択された言葉を被認証者に提示し、提示した言葉を被認証者に発声させて声紋を解析し、解析結果と基本単位の声紋データから生成された声紋データとを照合して、両者が一致した場

合にその被認証者を個人認証することを特徴とする。

【００１６】上記方法によれば、基本単位の声紋データを選択された言葉の配列に配列して声紋データを作成するため、声紋データを記憶しておくメモリ容量が少なくて済み、消費者を認証するための鍵となる「言葉」の選択が増える。また、消費者は基本単位の言葉を発声して登録するだけでよく、「言葉」は認証の都度、変えられることから、さらに高いセキュリティを維持することが可能である。

【００１７】前記記憶媒体から複数の言葉のうちの任意の１つを選択する際に、前記認証手段の内部に格納されている乱数発生プログラムを用いてもよい。

【００１８】上記方法によれば、セキュリティの鍵となる「言葉」を無秩序に選択することができるので、高いセキュリティを維持することが可能である。

【００１９】前記認証手段は、前記記憶媒体から複数の言葉のうちの任意の２つ以上を選択してもよい。

【００２０】本発明の個人認証システムは、被認証者が操作する第１の操作手段と、該被認証者の認証を要求する第２の操作手段と、該被認証者の認証を行う認証手段とが通信網を介して接続されているシステムにおいて、該認証手段は、少なくとも、被認証者単位で複数の言葉とそれらの言葉を被認証者に発声させたときの声紋データを予め記憶させておく記憶媒体と、被認証者が第１の操作手段から入力した該被認証者のＩＤデータが通信網を介して該認証手段に伝えられたときに、該記憶媒体から、該ＩＤデータに対応する複数の言葉のうちの任意の１つとそれに対応する声紋データを選択して選択された言葉を該通信網を介して被認証者に提示する手段と、提示した言葉を被認証者が発声した声を通信網を介して入力して声紋を解析する解析手段と、解析結果と該記憶媒体から選択された声紋データとを照合する照合手段とを有することを特徴とする。

【００２１】上記構成によれば、消費者を認証するための鍵となる「言葉」を、例えば日時等により認証手段側で任意に変えることができ、デパートメントストアや商店、自動販売機、銀行のＡＴＭ等の公共の場所であって、悪意を有する者が存在するおそれがある場所においても、高いセキュリティを維持することが可能である。

【００２２】本発明の個人認証システムは、被認証者が操作する第１の操作手段と、該被認証者の認証を要求する第２の操作手段と、該被認証者の認証を行う認証手段とが通信網を介して接続されているシステムにおいて、該認証手段は、少なくとも、複数の言葉を含む一覧データ表と被認証者の基本単位の声紋データを予め記憶させておく記憶媒体と、被認証者が第１の操作手段から入力した該被認証者のＩＤデータが通信網を介して該認証手段に伝えられたときに、該記憶媒体から、該一覧データ表に含まれた複数の言葉のうちの任意の１つを選択すると共に、入力されたＩＤデータに対応する基本単位の声

紋データを選択された言葉の配列に配列して声紋データを生成して、選択された言葉を該通信網を介して被認証者に提示する手段と、提示した言葉を被認証者が発声した声を通信網を介して入力して声紋を解析する解析手段と、解析結果と基本単位の声紋データから生成された声紋データとを照合する照合手段とを有することを特徴とする。

【００２３】上記構成によれば、基本単位の声紋データを選択された言葉の配列に配列して声紋データを作成するため、声紋データを記憶しておくメモリ容量が少なくて済み、消費者を認証するための鍵となる「言葉」の選択が増える。また、消費者は基本単位の言葉を発声して登録するだけでよく、「言葉」は認証の都度、変えられることから、さらに高いセキュリティを維持することが可能である。

【００２４】前記認証手段は、前記記憶媒体から複数の言葉のうちの任意の１つを選択する際に使用する乱数発生プログラムが内部に格納されていてもよい。

【００２５】上記構成によれば、セキュリティの鍵となる「言葉」を無秩序に選択することができるので、高いセキュリティを維持することが可能である。

【００２６】前記認証手段は、前記記憶媒体から複数の言葉のうちの任意の２つ以上を選択してもよい。

【００２７】

【発明の実施の形態】以下に、本発明の実施の形態について、図面を参照しながら説明する。

【００２８】（実施形態１）図1は、本発明の一実施形態である個人認証システムの構成を示すブロック図である。ここでは、個人認証に関る部分のみを示しており、少なくとも消費者が操作を行う第１の操作端末２１４、事業者が操作を行う第２の操作端末２１３、認証機関が操作を行うサーバー（ホストコンピューター）、およびこれらを結ぶインターネット等の通信網２１７から構成されている。

【００２９】第１の操作端末２１４は、消費者側に設けられるものである。例えば、携帯電話に代表される移動通信端末やパーソナルコンピュータの端末等が挙げられる。

【００３０】この第１の操作端末２１４は、図２に示すように、少なくともＭＰＵ２３１と、消費者が発声する音声を入力するためのマイクロホン２３３と、マイクロホン２３３から取り込んだ音声をデジタル信号に変換するＡ／Ｄ変換手段を含む音声処理部２３２と、デジタル化した音声デジタルを一旦記憶させるメモリ２３２ａと、電子商取引プログラムを格納した領域２３４ａ、認証処理を行うための認証サーバー（ホストコンピューター）２１５とやり取りを行うための認証通信処理プログラムを格納した領域２３４ｂを含むメモリ領域２３４から構成され、これらがバスライン２３０により接続されている。なお、メモリ領域２３４ｃおよび２３４ｄにつ

いては後述するが、本実施形態では省略可能である。

【００３１】また、第２の操作端末２１３は、例えば自動販売機やオンラインショッピングを行う商店（インターネット上の仮想商店も含む）、チケットや宿泊等の予約を行うための操作端末等が挙げられる。

【００３２】この第２の操作端末２１３は、図３に示すように、少なくともＭＰＵ２２１と、例えば商品の品番、仕様、その販売価格や商品画像等の商品情報一覧を格納したデータメモリ領域２２２と、電子商品取引プログラムを格納した領域２２３ａを含むメモリ領域２２３から構成され、これらがバスライン２２０により接続されている。

【００３３】なお、上記第１の操作端末２１４の機能と第２の操作端末２１３の機能が融合されて１つの操作端末を構成していてもよい。例えば自動販売機やオンラインショッピングを行う商店（インターネット上の仮想商店も含む）、チケットや宿泊等の予約を行うための操作端末、銀行のキャッシュディスペンサ等が挙げられる。

【００３４】さらに、認証機関のサーバー（ホストコンピューター）２１５は、図４に示すように、少なくともＭＰＵ２４１と、複数の言葉とその言葉の肉声に由来する声紋からなる組み合わせデータが格納されているデータメモリ領域２４２と、第１の操作端末２１４から受信したデジタル化された音声データから声紋を抽出し、データメモリ領域２４２に格納されているデータと照合解析する音声処理解析部２４４と、電子商取引プログラムを格納した領域２４３ａ、第１の操作端末２１４や第２の操作端末２１３とやり取りを行うための認証通信処理プログラムを格納した領域２４３ｂ、上記音声処理解析を行って認証を行うための認証可否処理プログラムを格納した領域２４３ｃを含むメモリ領域２４３から構成され、これらがバスライン２４０により接続されている。なお、メモリ領域２４３ｃおよび２４３ｄについては後述するが、本実施形態では省略可能である。

【００３５】以下に、本実施形態の個人認証システムにおける、商品購入や予約等を希望する消費者の個人認証を含む処理手順について、図５のフローチャートを参照しながら説明する。まず、ステップ２０１において、消費者は第１の操作端末２１４を操作し、インターネット等の通信網２１７を経由して事業者（商店等）に備えられた第２の操作端末２１３に働きかけて、データメモリ領域２２２に格納されている商品の品番、仕様、その販売価格や商品画像等の商品情報一覧を参照して、所望の商品と数量（以後、商品情報と称する）を選択する。

【００３６】次に、ステップ２０２において、第２の操作端末２１３は、確認のために第１の操作端末２１４に受信した消費者からの商品情報にその購入金額を加えた情報を第１の操作端末２１４に返送する。

【００３７】続いて、ステップ２０３において、消費者は第１の操作端末２１４により、第２の操作端末２１３から送信されてきた商品情報とその購入金額を確認する。そして、消費者はその内容に問題があれる場合には不承認としてステップ２０１に戻し、一方、内容に問題が無い場合には承認して次のステップ２０４に進む。

【００３８】ステップ２０４では、消費者は承認した商品情報とその購入金額と共に、消費者を識別するＩＤ番号（暗証番号やパスワード等、但し、第１の操作端末２１４が携帯電話等であって、予め電話番号等、ＩＤに相当するものが登録されている場合には、暗証番号やパスワードをさらに入力力することを省略することができる。）を第１の操作端末２１４から認証機関側に備えられたサーバー２１５に送信する。なお、ＩＤ番号（数字）の代りにアルファベット等の英数字を用いてもよい。

【００３９】その後、ステップ２０５において、サーバー２１５は、内蔵している記憶媒体（データメモリ領域２４２）から消費者固有のＩＤ番号を検索する。そして、サーバー２１５は、消費者から入力されたＩＤ番号が記憶媒体に記憶されていない場合には以降の処理を拒否してステップ２０４に戻し、一方、ＩＤ番号が記憶媒体に記憶されている場合にはステップ２０６に進む。

【００４０】ステップ２０６では、サーバー２１５は、データメモリ領域２４２から、消費者固有のＩＤ番号に対応したセキュリティの鍵として活用する複数の暗証コード（例えば「山」、川等の言葉と、その言葉を消費者が発声した際の声紋データとの組み合わせ）の中から１組の暗証コードを選択する。これらの複数の暗証コードは、ＩＤ番号と共に、予めデータメモリ領域２４２に登録しておく。このときの暗証コード（言葉）の選択の仕方は、悪意を有する者にとって予測困難であるように選択するのが好ましい。例えば、サーバー内にタイマー機能を設けることにより、複数の暗証コードの中から選択される暗証コードを変えることができる。さらにセキュリティを向上させるためには、例えば、サーバー２１５内に乱数発生プログラム等を内蔵させ（例えばメモリ２４３に格納し）、これを利用して複数の暗証コードの中から１つの暗証コードを選択することができる。

【００４１】次に、ステップ２０７において、サーバー２１５は、データメモリ領域２４２から選択した１組の暗証コード（「言葉」とその言葉を消費者が発声した際の声紋データ））を、消費者側に備えられた第１の操作端末２１４へ送信する。

【００４２】送信された「言葉」は、例えば第１の操作端末２１４の画面（図示せず）に表示される。続いて、ステップ２０８において、消費者は画面に表示された「言葉」を第１の操作端末２１４のマイクロホン２３３に向かって発声する。第１の操作端末２１４の音声処理部２３２は、入力された「言葉」をＡ／Ｄ変換してデジタル化し、そのデジタル音声データをサーバー２１５に送信する。その後、ステップ２０９において、サーバー

２１５は受信した消費者が発声したデジタル音声データを音声処理解析部２４４により声紋データに変換し、この声紋データと先のステップ２０６で選択されたデータメモリ領域２４２内の声紋データとを比較する。そして、サーバー２１５は声紋データが不一致である場合はステップ２０８に戻し、一方、一致している場合には本人であると認証して、事業者側に備えられた第２の操作端末（第２の操作端末が含まれているものであってもよい）２１３にその結果を送信する。

【００４３】これにより、図示はしていないが、次のステップとして、事業者は消費者への商品の発送手続きまたはチケット発売や予約手続き、或いは銀行のキャッシュディスペンサであれば引出処理等を行うと共に、それに要した代金をプリペイドカード（インターネット上の仮想プリペイドカードも含む）からの引き落としたり、またはサーバー２１５を通じて金融機関に代金を通知して消費者の講座からの引き落としや振り込み処理を行って、事前または事後に、消費者から商品の購入代金を事業者の口座等に払い込ませる。

【００４４】さらに、セキュリティを強化するためには、ステップ２０８において、消費者が発声した「言葉」をデジタル変換した後、第１の操作端末２１４のメモリ２３４に格納された暗号化処理プログラム２３４ｃを活用して暗号化して、サーバー２１５に送信する手法も有効である。この場合、サーバー２１５は受信した音声デジタルをメモリ２４３に格納された復号化処理プログラム２４３ｄを活用して復号してから声紋データに変換する。そして、サーバー２１５は、データメモリ領域２４２に記憶された複数の暗証データの中から１組の暗証コード（「言葉」とその声紋データ）を選択し、その選択された暗証コードの「言葉」をメモリ領域２４２ｅに格納されている暗号化処理プログラムを活用して暗号化して、消費者側に備えられた第１の操作端末２１４へ送信する。第１の操作端末２１４は、メモリ領域２３４ｄに格納されている復号化処理プログラムを活用して「言葉」に復号し、画面に表示することができる。

【００４５】なお、本実施形態では１組の暗証コードを選択した例について説明したが、セキュリティを高めるためには、複数の暗証コードを選択して組み合わせてもよい。例えば、複数の暗証コードを選択して組み合わせる場合には、複数の暗証コードの「言葉」を消費者側の第１の操作端末２１４に送信して消費者に複数の言葉を発声させるようにする。さらに、認証不一致により再度認証を試みる場合に、選択される「言葉」を変えるようにしてもよい。

【００４６】（実施形態２）以下に、本実施形態の個人認証システムにおける、商品購入や予約等を希望する消費者の個人認証を含む処理手順について、図６のフローチャートを参照しながら説明する。本実施形態では、上記実施形態１と異なり、サーバー２１５の記憶媒体（データメモリ領域２４２）に消費者が発声した言葉（意味のある言葉としての声紋データ）を記憶しておかず、認証機関が用意した言葉、例えば「山」、「川」、・・・等の言葉の一覧データ表と、消費者が発声した基本単位（５０音）の声紋データ、例えば「あ、い、う、え、お、・・・」等の声紋データのみを記憶しておく。

【００４７】ステップ３０１～ステップ３０５までは、上記実施形態１のステップ２０１～ステップ２０５と同様であるので、ここでは説明を省略する。

【００４８】ステップ３０６では、消費者が入力したＩＤ番号がサーバー内の記憶媒体（データメモリ領域２４２）に記憶されていることを確認したサーバー２１５は、データメモリ領域２４２から、認証機関が用意した言葉の一覧データ表からランダムに１つの言葉を選択する。これは、上記実施形態１とは異なり、消費者のＩＤ番号に依存した暗証コードではない。このときの言葉の選択の仕方は、悪意を有する者にとって予測困難であるように選択するのが好ましく、例えば、サーバー２１５内に乱数発生プログラム等を内蔵させ、これを利用して言葉の一覧データ表から１つの言葉を選択することができる。

【００４９】次に、ステップ３０７では、、消費者固有のＩＤ番号に対応してデータメモリ領域２４２に記憶されている基本の声紋データを、選択された「言葉」に対応した声紋の配列に配列して、声紋データを生成する。

【００５０】続いて、ステップ３０８において、サーバー２１５は、データメモリ領域２４２から選択した「言葉」を、消費者側に備えられた第１の操作端末２１４へ送信する。

【００５１】送信された「言葉」は、例えば第１の操作端末２１４の画面（図示せず）に表示され、または音声出力される。続いて、ステップ３０９において、消費者は画面に表示され、または音声出力された「言葉」を第１の操作端末２１４のマイクロホン２３３に向かって発声する。第１の操作端末２１４の音声処理部２３２は、入力された「言葉」をＡ／Ｄ変換してデジタル化し、音声処理部内のメモリ領域２３２ａに一旦記憶した後、暗号化処理等を行い、そのデジタル音声データをサーバー２１５に送信する。

【００５２】その後、ステップ３１０において、サーバー２１５は受信した消費者が発声したデジタル音声データを音声処理解析部２４４により声紋データに変換し、この声紋データと先のステップ３０７で生成された声紋データとを比較する。

【００５３】その後の認証可否と、本人認証後の処理は上記実施形態１と同様であるので、ここでは説明を省略する。

【００５４】さらに、セキュリティを強化するためには、ステップ３０９において、消費者が発声した「言葉」をデジタル変換した後、第１の操作端末２１４のメ

モリ２３４に格納された暗号化処理プログラム２３４ｃを活用して暗号化して、サーバー２１５に送信する手法も有効である。この場合、サーバー２１５は受信した音声デジタルをメモリ２４３に格納された復号化処理プログラム２４３ｄを活用して復号してから声紋データに変換する。そして、サーバー２１５は、データメモリ領域２４２に記憶された言葉の一覧データ表から１つの「言葉」を選択し、その選択された「言葉」をメモリ領域２４２ｅに格納されている暗号化処理プログラムを活用して暗号化して、消費者側に備えられた第１の操作端末２１４へ送信する。第１の操作端末２１４は、メモリ領域２３４ｄに格納されている復号化処理プログラムを活用して「言葉」に復号し、画面に表示し、またはスピーカー（図示せず）から音声出力することができる。

【００５５】なお、本実施形態では１つの言葉を選択した例について説明したが、セキュリティを高めるためには、複数の「言葉」を選択して組み合わせてもよい。さらに、認証不一致により再度認証を試みる場合に、選択される「言葉」を変えるようにしてもよい。

【００５６】

【発明の効果】以上詳述したように、本発明によれば、消費者を認証するための鍵となる「言葉」を、例えば日時等により認証手段側で任意に変えることができるので、デパートメントストアや商店、自動販売機、銀行のＡＴＭ等の公共の場所であって、悪意を有する者が存在するおそれがある場所においても、高いセキュリティを維持することができる。

【００５７】さらに、他の本発明によれば、被認証者の基本単位の声紋データのみを認証手段（サーバー）内に記憶させ、選択された言葉の配列に配列して声紋データを作成するため、声紋データを記憶しておくメモリ容量が少なくて済み、消費者を認証するための鍵となる「言葉」の組み合わせを増やすことができるため、選択可能な「言葉」を増やすことができる。また、消費者は基本単位の言葉を発声して登録するだけでよく、「言葉」は認証の都度、変えられることから、さらに高いセキュリティを維持することができる。

【００５８】従って、消費者はクレジットカードやデビットカード等を携帯する必要がなくなる。

【図面の簡単な説明】

【図１】本発明の一実施形態である個人認証システムの構成を説明するためのブロック図である。

【図２】本発明の実施形態に係る第１の操作端末の構成を説明するためのブロック図である。

【図３】本発明の実施形態に係る第２の操作端末の構成を説明するためのブロック図である。

【図４】本発明の実施形態に係る認証手段（サーバー）の構成を説明するためのブロック図である。

【図５】実施形態１の個人認証方法について説明するためのフローチャートである。

【図６】実施形態２の個人認証方法について説明するためのフローチャートである。

【図７】従来の個人認証システムの構成を説明するためのブロック図である。

【符号の説明】

１０　インターネット
１１　商店の端末装置
１２　パーソナルコンピュータ
１３　認証サーバー
１３ａ　解読回路
１３ｂ　特徴抽出処理回路
１３ｃ　ＭＰＵ
１３ｅ　メモリ
１４　ＭＰＵ
１５　メモリ
１５ａ　電子商取引プログラム
１５ｂ　認証通信処理プログラム
１５ｃ　暗号化処理プログラム
１５ｄ　認証データ生成プログラム
１６　音声入力装置
１６ａ　メモリ
１３１　ＩＤパターン記憶部
１３２　標準ＩＤパターンテーブル
１３３　ＤＰマッチング処理プログラム
１３４　データ送信プログラム
２１３　第２の端末装置
２１４　第１の端末装置
２１５　認証機関（サーバー）
２１７　通信網
２２０　バスライン
２２１　ＭＰＵ
２２２　データ（データメモリ領域）
２２３　メモリ
２２３ａ　電子商取引プログラム（格納領域）
２３０　バスライン
２３１　ＭＰＵ
２３２　音声処理部
２３２ａ　メモリ
２３３　マイクロホン
２３４　メモリ
２３４ａ　電子商取引プログラム（格納領域）
２３４ｂ　認証通信処理プログラム（格納領域）
２３４ｃ　暗号化処理プログラム（格納領域）
２３４ｄ　復号化処理プログラム（格納領域）
２４０　バスライン
２４１　ＭＰＵ
２４２　データ（データメモリ領域）
２４３　メモリ
２４３ａ　電子商取引プログラム（格納領域）
２４３ｂ　認証通信処理プログラム（格納領域）

13

２４３ｃ　認証可否処理プログラム

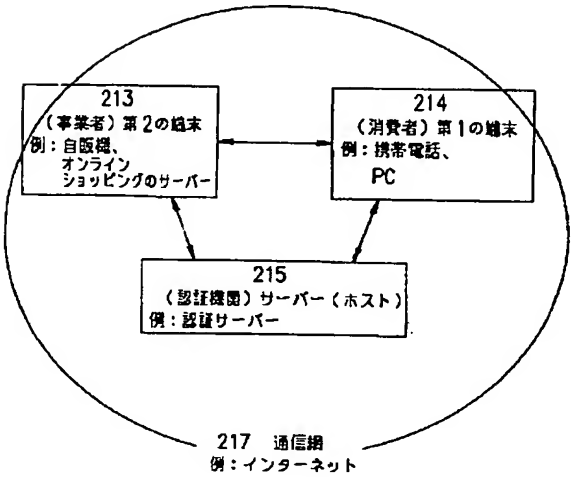
２４３ｅ　暗号化処理プログラム（格納領域）

14

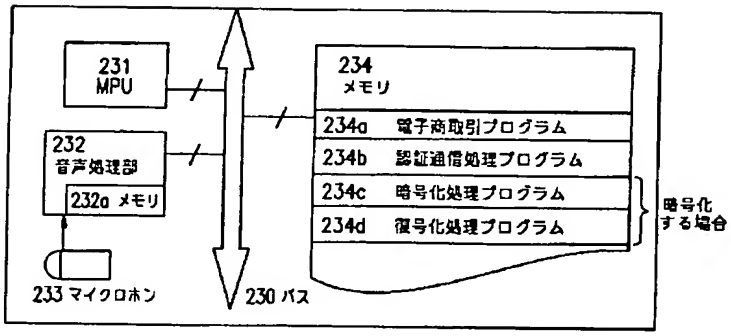
２４３ｄ　復号化処理プログラム（格納領域）

２４４　音声処理解析部

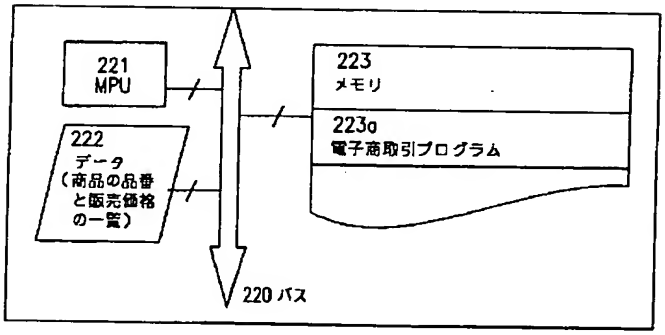
【図１】



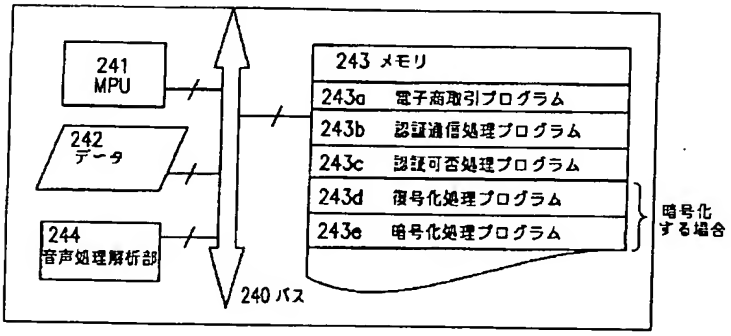
【図２】



【図３】



【図４】



【図７】